- The security features that were identified by the members, supplier and distributors in their workshop sessions. These are the characteristics of the portal that must be present in order to meet their CTQs.

- Additional features that were identified in follow-up review sessions with supply chain coordinator personnel. These are more subtle features that emerged during technical, organizational and authorization discussions.

- Best practices that are frequently employed in system security and access management.

Each functional component will first be described in terms of purpose and general approach. Then details will be provided for each function to specify the capabilities that must be present.

Assuming that the supply chain coordinator desires to use existing 3rd party software as much as possible, the traditional approach of specifying inputs, processing and outputs for each function will not be strictly followed here. Rather, the emphasis will be placed on clearly describing the full set of capabilities that will be required to deliver the features needed to meet the CTQs. The details associated with the specifics of inputs, forms, detailed processing and outputs will vary by vendor and the vendor's approach to providing the necessary capabilities. It will be the job of the vendors to provide these details so that the supply chain coordinator can use them to determine the best approach for their requirements.

Logon (Authentication)

Function Purpose

The logon function represents the first line of security and it validates that a user is authorized to access the portal.

Function Details

The authentication process begins when a user connects to the portal. At that time they will be prompted for:

- Company ID
- User ID
- Password

The user will enter the requested data and it will be encrypted prior to sending it to the portal logon function. Additionally the password field will be masked when the user enters it (i.e. it won't print on the screen when the user enters it).

Once the user has submitted the information, the logon function will check the portal access control list to determine if access is permitted to the companyID/userID/password combination that the user submitted.

Users failing to enter a valid companyID/userID/password combination will be notified of the failure and re-prompted. A userID will be locked out after n failures.

The logon function will provide the following password management capabilities:

- Password disablement after an administrator specified period of inactivity.
- New user must provide a new password the first time they logon to the portal.
- Passwords will expire after an administrator specified period of time and the user will be required to provide a new one.
- Alternate passwords will be provided for lost/forgotten password situations.

New passwords will be subjected to minimum security password validation rules. These will include things like minimum/maximum length, percent of characters that must differ, uniqueness, etc.

Once a user has been successfully authenticated the system will:

- Offer an option to the user to change their password
- Show the date and time the user last sign on to the system (detect stolen user ID and password).
- Retrieve the user's profile data that defines what data and functions the user can access and transfer to the policy management function (i.e. portal main menu).

All details associated with the logon session will be written to the audit log.
The system administrator will be notified of user ID lockout. The following table lists User Specified Features.

Table 9

Feature	**CTQ Category**	**Explanation**
Lockout user after n unsuccessful logon attempts	Security, Prevention	
Notify administrator of lockouts	Security, Prevention	This is a proactive notification that occurs via email, pager, etc. when the attempt occurs
On line monitoring	Security, Prevention	This includes administrator notification of lockout and

Feature	CTQ Category	Explanation
		could be expanded to include other threats or situations.
Provide alternate passwords for lost/forgotten password situations	Flexibility	
Password expiration; require periodic password changes	Security, Prevention	
Acceptable password length parameters	Security	
Ability to assign/select password	Security	User can specify their password and change it any time.
Ability to transfer logon intelligence.	Simplicity	The ability to transfer the user profile information that specifies what data and applications they can access is helpful for supporting a single sign on capability for the portal.
Record all activities to the audit log	Security, Prevention, Reporting	This was not an explicitly stated feature. However, it will be required to support the reporting features that were requested by the users.

Community Management

The community management capability allows administrators to manage the user activities within the portal. Specifically it provides the capabilities to add, change and delete users, and to manage what the user can see and what functions they can perform.

Community management can be covered in four sections:

- *Community/Domain Wide Administration*

  Describes the supply chain coordinator system wide administrative capabilities that will be required to establish the community and the entities that make it up (i.e. members, suppliers, distributors and supply chain coordinator).

- *Basic Delegated Community Management*

  Describes the capabilities that will be needed to achieve the CTQs. Many of the capabilities that are found in this basic model can be accommodated by 3rd party software. Some custom programming will likely be required to manage authorization within the complex organizational structures found at the supply chain coordinator.

- *Group Hierarchical Management*

  Describes the use of hierarchies to manage access. This will achieve many of the simplicity and flexibility related CTQs that were not meet by the basic model. It will likely require custom development.

- *Data Publication*

  Describes a capability that is need to support situations such as joint ownership of stores and corporate board committees. It will enable the owner of a group to permit user in other groups to access data in the owner's group. This will be largely custom development.

Community/Domain Wide Administration

Function Purpose

There are certain capabilities that affect the entire community or all of the occupants of a domain (members, suppliers, distributors and supply chain coordinator). These are limited to a single system wide administrator and potentially to domain administrators.

Function Details

Community and domain wide administration will include the following capabilities:

- *Community wide administration*
  - Add/change or delete a domain.
  - Delegate domain administration to a domain administrator.

- *Domain administration*

  Domains are comprised of organizations (e.g. members). Organizations are made up of data related entities (retailers, distribution center, plants, etc.). The domain administrator needs the following capabilities to create and manage organizations that make up their domain.

  - Add, change and delete data related entities (e.g. retailers).
  - Link data related entities together (e.g. retailers) into an organization (e.g. member).
  - Create an organization administrator and delegate the administration of their organization to them.

Basic Delegated Community Management

Function Purpose

The purpose of community management is to provide a sub administrator with the ability to control what their users can view and what tasks they can perform.

An administrator who has been granted administrative privileges for the sub domain that represents their organization performs community management (e.g. a member's retail outlets make up the member's sub domain).

The basic model provides the administrator with tools that are used to manage a user's access (view and tasks). These tools include:

- Groups to specify span of control.
- Privileges to specify tasks.
- Roles to specify a set of privileges that are associated with a function (e.g. retail outlet manager).

Community management then provides the administrator with the ability to add, change and delete users.

Lastly it enables the administrator to control user's view and access rights by associating them with a group of data related entities (e.g. retailer) to specify what the user can see and with a role or specific privileges to specify what tasks the user can perform.

Figure **74** is a flow diagram showing how group and roles manage access. User ABC **7402** is associated with Group 2 and is assign a manager role. This entitles ABC to order F and P and view forecasts for retail outlets 1 and 2.

Function Details

Functional details will be covered in the context of groups, roles and users.

Group Management

As stated earlier, a group is an organizational entity that is made up of one or more data related entities. The retail outlets owned by a franchisee comprise a member group. Groups serve to specify a user's span of control when they are associated with a user.

An administrator who has been authorized to manage groups can create new groups, and change and delete existing groups.

New groups:

- Requires an ID that is unique in the administrator's span of control.
- Requires a descriptive name.
- Entities (e.g. retailers) that are placed in the new group must exist within the administrator's span of control.

In order to change or delete a group, it must exist in the administrator's span of control. Entities being added to an existing group (change) must exist in the administrators span of control.

Role Management

A role is a functional entity that is made up of tasks the function is permitted to perform. A restaurant manager is a role that is permitted (i.e. given a privilege) to perform the tasks of ordering food and packaging, and viewing forecasts.

An administrator who has been authorized to manage roles can create new roles, and change and delete existing ones.

An administrator must possess any privilege they assign to a role.

New roles:

- Requires an ID that is unique in the administrators span of control.

- Requires a descriptive name

In order to change or delete a role, it must exist in the administrator's span of control.

Privileges can be specified as default or optional when they are assigned to a role. Default privileges are automatically given to a user when they are assigned to a role. The administrator must explicitly specify each optional privilege (yes/no) for a user when they are assigned a role.

A role may be assigned to a group as well as to a user. When it is associated with a group, users receive the privileges specified by the role when they are associated with the group.

User Management

A user is an individual who is authorized to perform some set of tasks on behalf of a group (e.g. a set of retail outlets).

An administrator who has been authorized to manage users can create new users, and change and delete existing ones.

A company ID, a user ID and a password identify a user. The administrator cannot view the user password.

New users:

- Require a user ID that is unique in the sub domain (e.g. unique within a member organization).
- Require an email address.
- Require a descriptive information such as name and address name.
- The system will assign the password to a new user and inform them of it via email.

User span of control:

- The administrator specifies a user's span of control by associating the user with a group(s) that represent the desired span of control.
- The administrator can associate (add) and disassociate (remove) users with groups.
- In order modify a user's span of control, the user must exist within the administrator's span of control.
- In order associate a user with a group, the group must exist within the administrator's span of control.

User/group application access:

- The administrator specifies the application a user/group can perform by assigning roles/privileges to the user/group.
- The administrator can add and remove roles/privileges from users/ groups.
- In order assign a role to a user/group, the role must exist within the administrator's span of control.
- In order modify a user roles/privileges, the user must exist within the administrator's span of control.
- An administrator must possess any privilege they assign to a user/group.
- If a role is being assigned to a user/group, and if the role has optional privileges, the administrator will be shown the optional privileges and allowed to remove ones that they don't want to grant to the user.

Other

All details associated with community management activities will be written to the audit log.

A capability to link community management with the supply chain coordinator's member management system is required to eliminate duplicate data entry and keep the two systems synchronized.

5 A batch bulk load capability is required to enable user to export data from existing systems to set up their organization in the portal community.

Table 10

Feature	**CTQ Category**	**Explanation**
Distributed community administration	Flexibility	Users need to be able to manage their users and their access within the portal. They don't want to be dependent on the supply chain coordinator.
Ability to add, change and delete users.	Security, Flexibility	
Ability to assign access to users	Security, Flexibility	Specify span of control and privileges
Ability to create roles or level of users	Simplicity, Flexibility	
Ability to set up default levels of access	Simplicity, Flexibility	
Ability to clone and/or access rights	Simplicity, Flexibility	
Mass delete of users	Simplicity, Flexibility	Not provided as a part of community management.

Ability to copy a user ID	Simplicity, Flexibility	Provide to extent that a user's access attributes can be easily specified through groups and roles
Ability to export user load information from member backend.	Cost	Large member would like to use existing data to establish/maintain their organization in the portal.
User can be associated with multiple groups.	Flexibility	District manager A is a backup for district manager B. As a result, A will need to perform ordering district A and B and will need to be associated with both groups. Feature will also be required to support organizations such as finance who will need to view the data of several groups.

Hierarchy

Function Purpose

The basic community model that was outlined in the previous section supported authorization and access management for a flat single level organization. Although this can be adapted to support a multi-level organization, it falls short on the CTQs related to simplicity and flexibility. Specifically, the administrator must create groups to correspond to each span of control. This results in a single entity having to be included in several groups. For example, a single retailer may be included in a district, region and a corporate group. Administration in a scenario like this is complex and labor intensive. It becomes particularly cumbersome and error prone because things like an organization change (e.g.

new retail outlet) requires the modification of several groups (i.e. add it to district, region and corporate group).

A hierarchy provides a superior way to manage span of control and access. The hierarchy defines a company's organization. A user's span of control is set by associating them to the node of the hierarchy that corresponds to their position in the company. This association authorizes them to view the data associated with any entity that belong to the node to which they are assigned. In the case of a new retail outlet, assigning it to a manager also places it in the span of control of the manager's district and region mangers and the corporate CEO.

Hierarchies can also simplify the specification of user privileges by associating them to a hierarchy.

Although hierarchies introduce technical complexity, they greatly simplify administration in large and complex organizations.

The following outlines the requirement details associated with hierarchies.

Function Details

A hierarchy is made up of nodes where a node represents a business function (e.g. retail outlet manager, district manager, etc.). The bottom nodes of a hierarchy are associated with a data related entity (e.g. retail outlet is associated with a manager node/function). They are then grouped under nodes at successively higher levels (e.g. districts, regions, etc.). The top of the hierarchy is a single node (e.g. corporate). In a hierarchy an entity (e.g. retail outlet) will appear in the span of control of each successive parent node.

The following administrative capabilities are required to manage authorization and access with hierarchies.

Hierarchy Management

- Add a node

  Specify a parent node in a hierarchy and add a node beneath it.

- Delete a node

  Specify a node in a hierarchy and delete it. This also results in the deletion of any dependent nodes reporting to the node that was deleted.

- Move a node

  Specify a node in a hierarchy and move it and its dependents to another node (drag and drop).

- Associate a data entity with a node

  Specify a node in a hierarchy and associate a data related entity to it (e.g. retailer) with it. In this situation, no nodes can exist beneath the node specified. Also the data related entity must exist in the administrator's span of control.

- Disassociate a data entity with a node

  Specify a data related entity in a hierarchy structure and delete it from it parent node.

- Move a data entity from one node to another

  Specify a data related entity in a hierarchy structure and move it from its present parent node to a new parent node (drag and drop).

User Span of Control Management

Span of control relates to the data a user can view. Under a hierarchy, associating a user to a node in a hierarchy specifies their span of control. This association entitles the user to view the data associated with any entity that is found in the user's node group.

User Access Management

Access management relates to the functions a user can perform. It is controlled by privileges and roles that are assigned to a user (groups of privileges). Under a hierarchy, roles and privileges can be associated to a node. Any user who is then associated to the node receives the privileges that accompany it. See the table below.

Table 11

Feature	**CTQ Category**	**Explanation**
Ability to publish rights and privileges across hierarchies.	Simplicity, Flexibility	
Ability to authorize multiple levels of a hierarchy	Simplicity, Flexibility	
Ability to manage access against hierarchies	Simplicity, Flexibility	
Flexible data access and management.	Simplicity, Flexibility	

Data Publication

Function Purpose

Portal data (e.g. a retailer) is owned by one and only one sub domain entity (e.g. member). The ability to view and process that data is restricted to users and groups who inhabit the entity's sub domain and who have been authorized to do so by its administrator.

However, there are several business situations where an organization needs to view and process data that is owned by another organization that may or may not belong to the same domain. Some common examples are:

- Two members share ownership of a retailer. As a result both members need to view information about the jointly held retail outlets and order supplies for them.

- Members belong to the supply chain coordinator board or corporate committees. In order to participate in these roles the members need to view and potentially access data in the supply chain coordinator's domain.

The data publication capability is a mechanism for the owners (e.g. member A) of an entity (e.g. retailer 123) to permit a users in another organization (e.g. member B) to view and access the entity's (i.e. retailer 123) data.

Function Details

Data publication is an administrative privilege. It is used by a data owner's administrator to setup a relationship with another party in the portal that will allow that party to view and access data entities (e.g. retailers) that are found the owner's sub domain.

The data publication function will possess the following capabilities.

- The administrator can add, change or delete a data publication relationship.

- Any data entity that is published must exist in the administrator span of control.

- The following elements will be provided to specify a data publication relationship.

    - The span of control (view) that is associated with a data publication. The span of control may be specified as an individual entity (e.g. a retailer), a group (e.g. a district) or a hierarchical node (if a hierarchy feature is provided).

- Privileges or functions the receiver can perform with the published data.

- The domain (i.e. member, supplier, distributor, supply chain coordinator) and sub-domain ID (company ID) of the organization to which the data is being published.

- The group or node ID in the receiving organization that the published data will be associated with.

- The user ID of the person in the receiving organization who will own the data. This person will control the user views and access (privileges) associated with the published data in their organization.

- All details associated with creating or modifying a data publication relationship will be written to the audit log.

The following table sets forth User Specified Features:

Table 12

Feature	**CTQ Category**	**Explanation**
User can view or access data in another sub-domain in their domain.	Simplicity Flexibility	Joint ownership of retail outlets by distinct members.
User can view or access data in different domain.	Simplicity Flexibility	Support board of directors and committees that require members to view and access supply chain coordinator corporate data.

Policy Enforcement

Function Purpose

The policy enforcement function is a centralized capability that manages access to all of the applications that comprise the portal.

Policies specify the access requirements for each application that makes up the portal. The policy enforcement function determines if a requesting user meets the access requirements for an application. The user is granted access by the policy enforcement function if they meet they requirements specified by the policy.

Function Details

A central administrative capability is required to maintain the policies that are used to manage access to the portal's applications.

The details associated with policy enforcement are as follows:

- When a user successfully logs on to the system by providing a valid user ID and password, their span of control and application privileges are retrieved.
- The user is presented with main menu for the portal.
- The user requests a function from the menu.
- The policy enforcement function retrieves the access policies for the requested application from the central policy repository.
- The user's span of control and application privileges are evaluated against the application's policies.

- If the user satisfies the requirements specified by the policy, access is granted.

- If the user does not satisfy the requirements specified by the policy, access is denied.

- Details associated with an access request are recorded in the central audit log.

- The policy enforcement function is responsible for interfacing with the portal applications and passing them information about the user that they require.

The following table sets forth User Specified Features.

Table 13

Feature	**CTQ Category**	**Explanation**
Single sign on	Simplicity	After signing on to the portal, the user can access all applications that make up the portal.
Ability to integrate with affiliates (i.e. other 3rd applications that make up the portal).	Simplicity Integration Cost	Provide the affiliate application with the user information it requires to function. Prevent redundant data entry, redundant security, etc.
Ability to interface with other applications: supply chain coordinator 3rd party Remote hosts	Simplicity Integration Cost	The supply chain coordinator wants to use 3rd parties and application service providers (ASPs) for their portal applications. The policy

Feature	CTQ Category	Explanation
Platform independent		enforcement manager must be capable of interfacing with a variety of platforms in a variety of situations.
Centralized policy management	Simplicity Integration Cost	Don't want redundant application access permission management.

Reporting

Function Purpose

The portal must provide its administrators with two forms of reporting:

- Community management reports.
- An event reporting capabilities that provides the administrator with the data and tools for researching issues, problems, potential breaches, etc.

Functional Details

The functional details of reporting will be covered from the perspective of report type.

Community Management Reports

Community management reports provide administrators with the information they need to manage their users, groups, roles and hierarchies (if implemented).

Reports will likely include:

- User information report showing things such as:

- Basic user information (name, address, telephone number, etc.)
- User span of control
- Roles/privileges
- Usage data (date of last logon, number of logons, total logon time, average logon time, etc.)
- User lockout

- Group reports showing thing such as:

  - The entities (e.g. retailers) that make up a group.
  - Role associated with a group.
  - Users associated with a group.

- Role reports showing things such as:

  - Default and optional privileges associated with each role.
  - Groups associated with each role.
  - Users assigned to each role.
  - Users assigned to each available privilege.

Report content will be limited by the administrator's span of control.

Query and filter capabilities will be required to specify report type and content (e.g. a specific group, a range of users, all roles, user usage details for date range, etc.).

Event Reporting

An event is a system activity that is written to the audit log. Examples of events include connection to the portal, logon attempt, application access requests, add a new user, system errors, etc. Information will accompany an events that identifies it, identifies the user that initiated it, the date and time the event was initiated, status (success/failure), etc.

Events are recorded so that the details associated with them are available to research problems, security breach attempts, etc.

An alert capability is required to specify administrator notification (email, page, etc.) in the case of certain events (e.g. attempted breach, a portal application is unavailable, etc.).

Because event reports from the audit log are run in response to problems or issues, good filtering capabilities will be required to eliminate unneeded data and provide the administrator with only the information they are seeking. Filters should include user(s), event, and date and time.

The following table sets forth User Specified Features.

Table 14

Feature	**CTQ Category**	**Explanation**
The following community management reports were identified: Master user list Click and view access list User with published data authorization (i.e. users in other domains or sub-domains. Usage reports	Security Reporting Prevention	
Lockout notification	Security	
Online monitoring capability	Security Reporting Prevention	
View audit log	Security	

Feature	CTQ Category	Explanation
	Reporting Prevention	
Parameter driven reports	Simplicity	

Technology

Component and Actor definition of the supply chain coordinator web portal

As detailed in the previous section, the supply chain coordinator's portal may allow access to supply chain applications. The nature of the applications require a feature and function set; this engagement collected CTQs and functions from the community and organized them along categories.

This section places a slightly different view of requirements on the portal. There may be a public site and a private site (secured access); there may also be applications behind the portal provided by 3rd party application service providers that fall under the private site. There may be administration pages to setup authentication and authorization policies. It is also a requirement that the portal support communications between the supply chain coordinator and the community and between community members.

System View Components

Some functional components that may comprise the Portal:

- PVC: Public View Component
- SVC: Secure View Component
- AC: Administrative Component
- CUC: Contact Us Component

A more detailed description of each of these components is stated in the following sections.

Public View Component

The Public View Component describes the functionality that is available to users of the public web pages on the supply chain coordinator portal.

Secure View Component

The Secure View Component describes the functionality that is available to users once they have logged onto the private pages of the supply chain coordinator portal. The private pages include access to the Applications and other functionality.

Administrative Component

The Administrative Component describes the functionality that allows users to access administrative links available to Company Administrators and individual Users. Additionally, the component contains information required for users to log on and request passwords.

Contact Us Component

The Contact Us Component describes the functionality and information that is available to users on both the public and private pages of the supply chain coordinator. This information consists of service-related questions and other areas of concern for community members.

Actor Definition

An actor is a user that plays a role with respect to the system. It is someone or something outside the application that interacts with the supply chain coordinator portal. The defined use cases and their definitions are specified below.

The systems 'Actors' are the different types of people involved in the business process. Earlier, several types of users are defined for each customer type (supply chain coordinator member, supply chain coordinator, supplier, distributor, retail outlet manager). While those are separate organizations, the actors in each share qualities at this high level of definition. The actors for the supply chain coordinator exchange portal are:

- Company Administrator (Tier 1 Registered User; Access to public and private pages)
- Exchange User (Tier 2 Registered User; Access to public and private pages)
- Non-Registered User (Tier 3; Access to public pages only)
- Content Manager (CM, Internal GXS/RM User who has permissions to submit updated content; Access to public and private pages)
- Internal Administrator (Internal GXS/RM User who has permissions to run reports validate the registration status of potential customers; Access to public and private pages)

Actor Details

Company Administrator; (Tier 1 Registered User; Access to public and private pages)

Description: A *Registered User (Tier 1)* is a registered community member who has Company Administrator responsibilities for their account.

Computer skills: Computer skill can vary, but a general knowledge of the Web is assumed.

Business Knowledge: Knowledge of products and services related to the supply chain coordinator suite of applications. This User may be responsible for setting up roles/responsibilities/permissions for Tier 2 Users in the account and company.

Exchange Level User; (Tier 2 Registered User; Access to public and private pages)

Description: A *Registered User (Tier 2)* is a registered user who has the second level of privileges. Tier 2 Users may use applications for which they are registered, but they may not sign up for additional applications without approval from their Tier 1 User.

Computer Skills: Computer skill can vary, but a general knowledge of the Web is assumed.
Business Knowledge: Knowledge of products and services related to a solutions suite of applications.

Non-Registered User; (Tier 3; Access to public pages only)

Description: A Non-*Registered User (Tier 3)* has access to the public pages of the supply chain coordinator. They may be able to register via their company administrator, (if the company has registered) or they may be able to register via the automated registration process (an option described in the upcoming sections). Until they are registered, Tier 3 users may not have any level of access to the private pages of the supply chain coordinator.

Computer Skills: Computer skill can vary, but a general knowledge of the Web is assumed.
Business Knowledge: Knowledge of products and services related to the solutions suite of applications.

Content Manager

Description: A *CM* is a Content Manager who has been authorized to add/update content to the portal, pertaining to the particular products they own.

Computer skills: Computer skill can vary, but a general knowledge of the Web is assumed.
Business Knowledge: Knowledge of products and services related to the solutions suite of applications.

Internal Administrator

Description: An Internal Administrator is a registered user who has been authorized to access certain report generation functionality on the private pages of the supply chain coordinator. They may be the only users allowed to view certain links related to report generation (Similar to Content Managers and the Upload Content Link).

Computer skills: Computer skill can vary, but a general knowledge of the Web is assumed.
Business Knowledge: Should be at the RailMarketplace.com, Inc. or GXS executive or marketing level, interested in site usage and feedback for further enhancements.

Portal Components and Requirement Index

The following section is an attempt to outline the requirements expressed by stakeholders/subject matter experts (SMEs) associated with the supply chain coordinator portal. These requirements revolve around the feature/function lists collected in meetings with the supply chain community as addressed in the previous sections. This list should be considered proposed at this point and based on GE's interpretation of the features collected. IT may be finalized through prioritization and solution decisions. It may be

further refined by the design process that the organization chosen to deliver this solution must complete during implementation.

A listing of these component areas along with their index key is provided below. Table 15 provides a listing of functional requirements so that they can be easily found.

Index Key

PVC: Public View Component

SVC: Secure View Component

AC: Administrative Component

CUC: Contact Us Component

Table 15

Req. ID	Requirement Name	Included in Approach
Public View Component		
UC-PVC.01	View Public Site	
UC-PVC.02	View supply chain coordinator press releases	
UC-PVC.03	View Service Info	
UC-PVC.04	View Media Coverage/Latest News	
UC-PVC.05	Request to Register	
UC-PVC.06	View Legal Pages (Extends from PVC.06)	
UC-PVC.07	View About Us	
UC-PVC.08	View Site Map	
UC-PVC.09	View FAQ's	
UC-PVC.10	Submit Feedback	
Secure View Component		
UC-SVC.01	View Secure Welcome Page	

UC-SVC.02	Select Application	
UC-SVC.03	Launch Application	
UC-SVC.04	View Application Request Form	
UC-SVC.05	Submit Application Request Form	
UC-SVC.07	View "Community Directory"	
UC-SVC.08	Search "Community Directory"	
UC-SVC.09	Community Directory- New User Listing	
UC-SVC.10	Submit Feedback	
UC-SVC.11	Submit User Survey	
UC-SVC.12	Register for Training	
UC-SVC.13	Quit Private Pages	
UC-SVC.14	View Press Releases	
UC-SVC.15	View Service Info	
UC-SVC.16	View Media Coverage/Latest News	
UC-SVC.17	View Site Map	
UC-SVC.18	View FAQ's	
Administrative Component		
UC-AC.01	Login	
UC-AC.02	Submit "Password" Reminder Request	
UC-AC.03	Re-set Password	
UC-AC.04	Submit "Administration" Change Request	
UC-AC.05	Add Content	
UC-AC.06	Submit "User Information" Change Request	
UC-AC.07	Generate User Report	
UC-AC.08	Generate Site Activity Report	
UC-AC.09	Clone User	
UC-AC.10	Mass Delete of Users	
UC-AC.11	Create and Manage Hierarchies	
UC-AC.12	Manages Access Rights Relative to Hierarchies	
UC-AC.13	Grant Privilege to Another User	

UC-AC.14	View Master User List	
UC-AC.15	View Access List	
UC-AC.16	View Users Who Can Access My Company's Data	
Contact Support Component		
UC-CUC.01	Submit Tech Support Feedback	
UC-CUC.02	View Tech Support Main Page	
UC-CUC.02	Access Email ASP	
UC-CUC.04	Submit Press Analyst Questions	
UC-CUC.05	View Business Development	
UC-CUC.06	Submit Billing Questions	
UC-CUC.07	Submit Accounts Payable Questions	
UC-CUC.08	Verify Account Information	
UC-CUC.09	Submit "Other" Questions	

Technology Options

Now that the features have been defined and categorized, and the portal components and actors are known, technology must be selected to address high priority items such as integrating affiliate sites, central policy management, and distributed user administration. Considerations for this selection may include the following IT strategy drivers:

Integrating existing and new security systems

- Integrating existing applications with new Web-based applications
- Providing a seamless integration between portal and affiliate sites
- Delegated and single-point administration
- Centralized security management
- Scalability of the integrated security systems

This list of general drivers matches up well to the feature list as collected:

- Distributed User Administration
- Administrative Audit Trail
- Access Management
- Logon/Password Management
- Reporting
- Policy Enforcement
- Data Management

Security is a major concern, as web sites may contain proprietary business information such as news, data/information, and procurement systems. Without adequate security, opportunities are presented for inappropriate dissemination of proprietary information, sabotage, and other mischievous acts.

Comprehensive Security for the supply chain community breaks down into three areas: Web, Network, and Security. Each of the features extends across all three areas, as the following chart illustrates.

Figure **75** is a schematic illustrating features **7502** and functions **7504** across web **7506,** network **7508** and system areas **7510.** Each area is very important to a strong security policy that may allow the supply chain coordinator to operate in a real-time integrated supply chain mode, but community management at the web layer was the main focus of this engagement and where most of the options and decisions need to be made.

Technically, from the web portal view, there are two main approaches to meeting the CTQs of the supply chain communities. The first option is for the supply chain coordinator to use its existing NT infrastructure. The second option involves purchasing a portal management solution to abstract user management from applications.